(1) 13

Original document

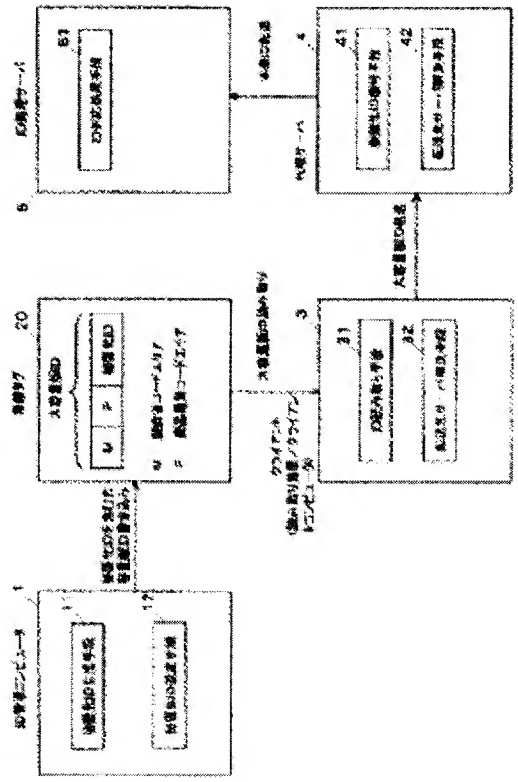
RADIO TAG SECURITY EXTENSION METHOD, ID MANAGEMENT COMPUTER SYSTEM, PROXY SERVER DEVICE, THEIR PROGRAMS, AND RECORDING MEDIUM OF PROGRAMS

Publication number: JP2004318645
Publication date: 2004-11-11
Inventor: KINOSHITA SHINGO; HOSHINO FUMISATO; KOMURO TOMOYUKI; FUJIMURA AKIKO
Applicant: NIPPON TELEGRAPH & TELEPHONE
Classification:
- international: ***G06K17/00; H04L9/32;*** **G06K17/00; H04L9/32;** (IPC1-7): G06K17/00; H04L9/32
- European:
Application number: JP20030113798 20030418
Priority number(s): JP20030113798 20030418

Abstract of **JP2004318645**

PROBLEM TO BE SOLVED: To protect privacy relating to the ID of a radio tag and to improve the security of the radio tag. SOLUTION: An ID management computer 1 conceals a small capacity version ID indicating an original product identification electronic code (EPC), turns it to a secret ID, sets it in the individual number area of the large capacity version ID of the radio tag 20, and sets information whose transmission destination is a proxy server 4 in the area of a manufacturer code and a product kind code. A client 3 reads the large capacity version ID from the radio tag 20 and transfers the large capacity version ID to the proxy server 4. The proxy server 4 restores the original small capacity version ID by decoding the secret ID set to the received large capacity version ID and transfers the decoded original small capacity version ID to an ID processing server 5 which processes the ID from the

manufacturer code and the product kind code.



JP2004318645: No description available

JP2004318645: No claims available

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-318645
(P2004-318645A)
(43)公開日　平成16年11月11日(2004.11.11)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06K 17/00	G06K 17/00	T	5B058
H04L 9/32	G06K 17/00	F	5J104
	H04L 9/00	673C	

審査請求 未請求　請求項の数 14　OL　（全 17 頁）

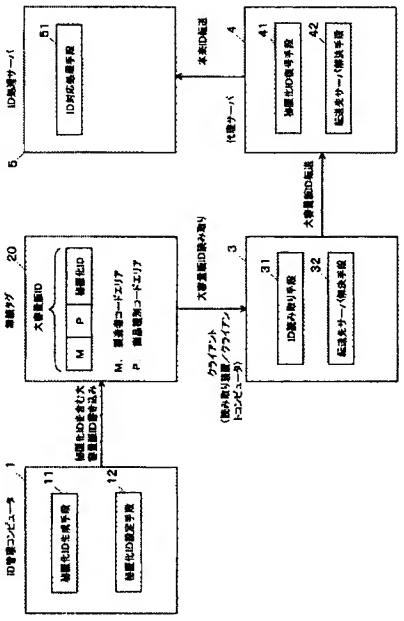
(21)出願番号　特願2003-113798(P2003-113798)
(22)出願日　平成15年4月18日(2003.4.18)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100087848
弁理士　小笠原　吉義
(74)代理人　100074848
弁理士　森田　寛
(74)代理人　100095072
弁理士　岡田　光由
(72)発明者　木下　真吾
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　星野　文学
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】無線タグセキュリティ拡張方法，ＩＤ管理コンピュータ装置，代理サーバ装置，それらのプログラムおよびそれらのプログラムの記録媒体

(57)【要約】
【課題】無線タグのＩＤに関するプライバシ保護を図り，無線タグのセキュリティを向上させる。
【解決手段】ＩＤ管理コンピュータ１は，本来の商品識別電子コード（ＥＰＣ）を示す小容量版ＩＤを秘匿化して秘匿化ＩＤとし，無線タグ２０の大容量版ＩＤの個体番号エリアに設定し，製造者コード，商品種別コードのエリアに代理サーバ４を送信先とする情報を設定する。クライアント３は，無線タグ２０から大容量版ＩＤを読み取り，代理サーバ４に大容量版ＩＤを転送する。代理サーバ４は，受信した大容量版ＩＤに設定されている秘匿化ＩＤを復号して本来の小容量版ＩＤを復元し，その製造者コード，商品種別コードからＩＤを処理するＩＤ処理サーバ５へ復号した本来の小容量版ＩＤを転送する。
【選択図】　図１



【特許請求の範囲】
【請求項1】
無線タグから読み取った識別コードを，その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおける無線タグセキュリティ拡張方法であって，
所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第１の識別コードを秘匿化したコードと，所定の代理サーバ装置を送信先として特定するための送信先特定情報とを含む第２の識別コードを生成し，無線タグに設定する過程と，
前記無線タグから第２の識別コードを読み取り，前記送信先特定情報を用いて前記代理サーバ装置へ第２の識別コードを送信する過程と，
前記代理サーバ装置において第２の識別コードから秘匿化された第１の識別コードを復号する過程と，
復号した第１の識別コードに含まれる送信先特定情報に基づいて特定のサーバ装置へ第１の識別コードを送信する過程とを有することを特徴とする無線タグセキュリティ拡張方法。
【請求項2】
無線タグから読み取った識別コードを，その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおける無線タグセキュリティ拡張方法であって，
所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第１の識別コードに，正当性認証用の認証子を付与したコードと，所定の代理サーバ装置を送信先として特定するための送信先特定情報とを含む第２の識別コードを生成し，無線タグに設定する過程と，
前記無線タグから第２の識別コードを読み取り，前記送信先特定情報を用いて前記代理サーバ装置へ第２の識別コードを送信する過程と，
前記代理サーバ装置において第２の識別コードに含まれる認証子から該識別コードの正当性を検証する過程と，
検証した結果，正当であると判定された場合に，前記第１の識別コードに含まれる送信先特定情報に基づいて特定のサーバ装置へ第１の識別コードを送信する過程とを有することを特徴とする無線タグセキュリティ拡張方法。
【請求項3】
無線タグから読み取った識別コードを，その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおける無線タグセキュリティ拡張方法であって，
所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第１の識別コードを秘匿化したコードと，正当性認証用の認証子と，所定の代理サーバ装置を送信先として特定するための送信先特定情報とを含む第２の識別コードを生成し，無線タグに設定する過程と，
前記無線タグから第２の識別コードを読み取り，前記送信先特定情報を用いて前記代理サーバ装置へ第２の識別コードを送信する過程と，
前記代理サーバ装置において第２の識別コードに含まれる認証子から該識別コードの正当性を検証する過程と，
検証した結果，正当であると判定された場合に，第２の識別コードから秘匿化された第１の識別コードを復号する過程と，
復号した第１の識別コードに含まれる送信先特定情報に基づいて特定のサーバ装置へ第１の識別コードを送信する過程とを有することを特徴とする無線タグセキュリティ拡張方法。
【請求項4】
請求項１，請求項２または請求項３記載の無線タグセキュリティ拡張方法において，

前記第１の識別コードは，商品識別電子コードであり，
前記送信先を特定するための送信先特定情報は，商品識別電子コードにおける製造者コードエリアまたはその製造者コードエリアと商品種別コードエリアとに設定される情報であることを特徴とする無線タグセキュリティ拡張方法。
【請求項5】
無線タグから読み取った識別コードを，その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおいて無線タグに識別コードを設定するＩＤ管理コンピュータ装置であって，
所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第１の識別コードを秘匿化したコードと，所定の代理サーバ装置であって前記秘匿化したコードを復号する代理サーバ装置を送信先として特定するための送信先特定情報とを含む第２の識別コードを生成する秘匿化識別コード生成手段と，
生成した第２の識別コードを，前記第１の識別コードによる識別対象となる個体に添付する無線タグに設定する秘匿化識別コード設定手段とを備えることを特徴とするＩＤ管理コンピュータ装置。
【請求項6】
無線タグから読み取った識別コードを，その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおいて無線タグに識別コードを設定するＩＤ管理コンピュータ装置であって，
所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第１の識別コードに，正当性認証用の認証子を付与したコードと，所定の代理サーバ装置であって前記認証子を用いて該識別コードの正当性を検証する代理サーバ装置を送信先として特定するための送信先特定情報とを含む第２の識別コードを生成する認証子付き識別コード生成手段と，
生成した第２の識別コードを，前記第１の識別コードによる識別対象となる個体に添付する無線タグに設定する認証子付き識別コード設定手段とを備えることを特徴とするＩＤ管理コンピュータ装置。
【請求項7】
無線タグから読み取った識別コードを，その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおいて無線タグに識別コードを設定するＩＤ管理コンピュータ装置であって，
所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第１の識別コードを秘匿化したコードと，正当性認証用の認証子と，所定の代理サーバ装置であって前記認証子を用いて該識別コードの正当性を検証するとともに前記秘匿化したコードを復号する代理サーバ装置を送信先として特定するための送信先特定情報とを含む第２の識別コードを生成する識別コード生成手段と，
生成した第２の識別コードを，前記第１の識別コードによる識別対象となる個体に添付する無線タグに設定する識別コード設定手段とを備えることを特徴とするＩＤ管理コンピュータ装置。
【請求項8】
無線タグから読み取った識別コードを，その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおける代理サーバ装置であって，
無線タグから識別コードを読み取った装置から，所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第１の識別コードを秘匿化したコードを含む第２の識別コードを受信する秘匿化識別コード受信手段と，
受信した第２の識別コードから秘匿化された第１の識別コードを復号する秘匿化識別コード復号手段と，
復号した第１の識別コードに含まれる送信先特定情報に基づいて特定のサーバ装置へ第１の識別コードを送信する識別コード転送手段とを備えることを特徴とする代理サーバ装置

。
【請求項9】
無線タグから読み取った識別コードを，その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおける代理サーバ装置であって，
無線タグから識別コードを読み取った装置から，所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第１の識別コードに，正当性認証用の認証子を付与したコードを含む第２の識別コードを受信する認証付き識別コード受信手段と，
受信した第２の識別コードに含まれる認証子から該識別コードの正当性を検証する識別コード検証手段と，
検証した結果，正当であると判定した場合に，前記第１の識別コードに含まれる送信先特定情報に基づいて特定のサーバ装置へ第１の識別コードを送信する識別コード転送手段とを備えることを特徴とする代理サーバ装置。
【請求項10】
無線タグから読み取った識別コードを，その識別コードに含まれる送信先を特定するための送信先特定情報に基づいて特定のサーバ装置へ送信するシステムにおける代理サーバ装置であって，
無線タグから識別コードを読み取った装置から，所定のコード体系によって無線タグの添付対象ごとに定められる前記送信先特定情報を含む第１の識別コードを秘匿化したコードと，正当性認証用の認証子とを含む第２の識別コードを受信する識別コード受信手段と，
受信した第２の識別コードに含まれる認証子から該識別コードの正当性を検証する識別コード検証手段と，
検証した結果，正当であると判定した場合に，前記第２の識別コードから秘匿化された第１の識別コードを復号する秘匿化識別コード復号手段と，
復号した第１の識別コードに含まれる送信先特定情報に基づいて特定のサーバ装置へ第１の識別コードを送信する識別コード転送手段とを備えることを特徴とする代理サーバ装置。
【請求項11】
請求項５，請求項６または請求項７記載のＩＤ管理コンピュータ装置が備える前記各手段をコンピュータによって実現するための，コンピュータに実行させるＩＤ管理コンピュータ装置用プログラム。
【請求項12】
請求項８，請求項９または請求項１０記載の代理サーバ装置が備える前記各手段をコンピュータによって実現するための，コンピュータに実行させる代理サーバ装置用プログラム。
【請求項13】
請求項５，請求項６または請求項７記載のＩＤ管理コンピュータ装置が備える前記各手段をコンピュータによって実現するための，コンピュータに実行させるプログラムを記録した
ことを特徴とするＩＤ管理コンピュータ装置用プログラムの記録媒体。
【請求項14】
請求項８，請求項９または請求項１０記載の代理サーバ装置が備える前記各手段をコンピュータによって実現するための，コンピュータに実行させるプログラムを記録したことを特徴とする代理サーバ装置用プログラムの記録媒体。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は，無線タグセキュリティ技術に関し，特に，無線タグを利用した自動認識システムにおいて，無線タグに関するプライバシ保護，無線タグの偽造／なりすまし防止を実現

する方法に関するものである。
【０００２】
【従来の技術】
商品などの自動認識システムを低コストで実現するために，無線タグに固有のＩＤ（識別コード）のみを格納し，それを商品に貼り付け，読み取り装置でＩＤを読み取り，商品関連情報は，ネットワーク側で管理するというアプローチが取られている。
【０００３】
例えば，米国のマサチューセッツ工科大学（ＭＩＴ）によるＡｕｔｏＩＤセンター（ｈｔｔｐ：／／ｗｗｗ．ａｕｔｏｉｄｃｅｎｔｅｒ．ｏｒｇ）では，商品のコード体系として，製造者コードと，商品の種別を示す商品種別コードと，商品個体の番号を示す個体番号とからなるＩＤを用い，そのＩＤだけを無線タグに格納し，商品関連情報を無線タグに格納したＩＤに関連付けてネットワーク上のコンピュータで管理することが考えられている。このシステムでは，商品関連情報に関するセキュリティは，ネットワーク側のセキュリティ技術を適用することにより確保されているが，無線タグのＩＤ読み取り制限などのセキュリティについては対処されていない（例えば，非特許文献１参照）。
【０００４】
【非特許文献１】
ＭＩＴ　ＡＵＴＯ－ＩＤ　ＣＥＮＴＥＲ，　”ＴＥＣＨＮＯＬＯＧＹ　ＧＵＩＤＥ”，［ｏｎｌｉｎｅ］，［平成１５年３月１８日検索］，インターネット＜ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ．ａｕｔｏｉｄｃｅｎｔｅｒ．ｏｒｇ／ｎｅｗ＿ｍｅｄｉａ／ｂｒｏｃｈｕｒｅｓ／Ｔｅｃｈｎｏｌｏｇｙ＿Ｇｕｉｄｅ．ｐｄｆ　＞
【０００５】
【発明が解決しようとする課題】
上記従来技術の方法では，無線タグからのＩＤ読み取り制限がなされておらず，読み取り装置を保有する者であれば誰でもＩＤを読み取ることができるため，消費者などの所有品情報が漏洩してしまうという問題がある。さらに，製造者コードや商品種別コードを入手できた場合，適当な商品個体コードを推測し無線タグに書き込むことによって，無線タグの偽造／なりすましにより容易に商品の偽造などが可能になってしまうといった問題もある。
【０００６】
本発明は，上記問題を解決するものであり，無線タグのＩＤ自体を秘匿化することにより，所有者のプライバシを保護する手段，および無線タグのＩＤに認証子を付加することにより，ＩＤの偽造／なりすましを防止する手段を低コストで提供することを目的とする。
【０００７】
【課題を解決するための手段】
本発明は，上記課題を解決するため，例えば以下の構成を採る。ここでは，無線タグに設定される識別コードとして商品識別電子コード（以下，ＥＰＣともいう）の例を用いて説明する。商品識別電子コードには，データ長が異なる小容量版ＩＤ（例：９６ビット）と大容量版ＩＤ（例：２５６ビット）の少なくとも２種類以上があり，それぞれ無線タグを添付する商品の製造者コードと，商品の種別を示す商品種別コードと，商品個体のシリアル番号を示す個体番号のエリアを有するものとする。
【０００８】
図１は，第１の本発明の構成の一例を示す図である。１はＩＤ管理コンピュータ，３は無線タグの読み取り装置または読み取り装置付きクライアントコンピュータ（以下，クライアントという），４はクライアント３およびサーバ５の双方と通信可能なコンピュータを備える代理サーバ，５はＩＤに基づくデータの加工や保管などの処理を行うコンピュータを備えるＩＤ処理サーバである。また，２０は商品に貼られる無線タグである。
【０００９】
ＩＤ管理コンピュータ１内において，１１は秘匿化ＩＤ生成手段，１２は秘匿化ＩＤ設定手段である。クライアント３内において，３１は無線タグ２０のＩＤ読み取り手段，３２

は転送先サーバ解決手段である。代理サーバ４内において，４１は秘匿化ＩＤ復号手段，４２は転送先サーバ解決手段である。ＩＤ処理サーバ５内において，５１はＩＤ対応処理手段である。

【００１０】

ＩＤ管理コンピュータ１は，秘匿化ＩＤ生成手段１１を利用し，本来の商品識別電子コードを示す小容量版ＩＤを秘匿化した秘匿化ＩＤを生成する。秘匿化ＩＤ設定手段１２は，生成した秘匿化ＩＤを無線タグ２０が有する大容量版ＩＤの個体番号のエリアに書き込み，また，大容量版ＩＤの製造者コードおよび商品種別コードのエリアに，代理サーバ４を送信先として特定することのできる商品情報とは無関係なコードを格納する。例えば製造者コードには，代理サーバ４を運営する第三者機関の会社コードを，商品種別コードには，ＩＤ秘匿化サービスを示すコードを格納する。

【００１１】

クライアント３は，ＩＤ読み取り手段３１により，無線タグ２０から秘匿化ＩＤを含む大容量版ＩＤを読み取り，ＩＤの製造者コードあるいは商品種別コードに基づき，転送先サーバ解決手段３２によって，アドレス解決サーバなどを別途利用するなどして，転送先サーバを決定する。もし，無線タグ２０から読み取ったＩＤが，秘匿化前の小容量版ＩＤであった場合には，ＩＤ処理サーバ５が転送先サーバとなるが，秘匿化ＩＤを書き込んで生成された大容量版ＩＤの場合には，製造者コード，商品種別コードから代理サーバ４が転送先サーバとして決定されることになる。なお，図１において図示省略したアドレス解決サーバは，あらかじめ定められた製造者コード，商品種別コードと，転送先サーバのアドレス（ＩＰアドレス等）とを対応付ける手段を持っており，製造者コード，商品種別コードによるアドレス解決要求に対して，製造者コード，商品種別コードから転送先サーバのアドレスを決定し，アドレス解決の要求元へ回答する。

【００１２】

クライアント３は，転送先サーバである代理サーバ４へ，秘匿化ＩＤを含む大容量版ＩＤを転送する。代理サーバ４は，受信した大容量版ＩＤの秘匿化ＩＤを，秘匿化ＩＤ復号手段４１により復号し，本来の小容量版ＩＤを生成し，転送先サーバ解決手段４２を用いて，小容量版ＩＤから解決される本来の転送先であるＩＤ処理サーバ５を決定し，小容量版ＩＤをＩＤ処理サーバ５へ転送する。ＩＤ処理サーバ５は，ＩＤ対応処理手段５１を用いて，ＩＤの保管や加工などの処理を行う。なお，クライアント３，代理サーバ４間の通信は認証，アクセス制御，暗号化など，何らかのセキュアな通信手段が提供されていることを前提としている。

【００１３】

ＩＤ管理コンピュータ１の秘匿化ＩＤ生成手段１１が，小容量版ＩＤの秘匿化を実現する方法としては，共通鍵暗号方式や公開鍵暗号方式を用いて暗号化する方法を用いることができる。この場合，代理サーバ４の秘匿化ＩＤ復号手段４１は，暗号化された小容量版ＩＤを共通鍵または秘密鍵を用いて復号する。また，小容量版ＩＤの秘匿化を実現する方法として，ＩＤ管理コンピュータ１と代理サーバ４との間で，任意に定めたユニークなコードと小容量版ＩＤとの対応情報をテーブル化して管理し，これらの対応情報を共有することにより，ＩＤ管理コンピュータ１では，小容量版ＩＤを任意のコードに置き換えることにより秘匿化し，代理サーバ４では，任意のコードから小容量版ＩＤを復号する方法を用いることもできる。

【００１４】

図２は，第２の本発明の構成の一例を示す図である。６はＩＤ管理コンピュータ，７はクライアント３およびＩＤ処理サーバ５の双方と通信可能なコンピュータを備える代理サーバ，２１は無線タグである。クライアント３，ＩＤ処理サーバ５は第１の本発明と同様である。また，ＩＤ管理コンピュータ６内の６１は認証子付きＩＤ生成手段，６２は認証子付きＩＤ設定手段であり，代理サーバ７内の７１は認証子付きＩＤ検証手段，７２は転送先サーバ解決手段である。

【００１５】

第２の本発明においては，ＩＤ管理コンピュータ６内の認証子付きＩＤ生成手段６１は，小容量版ＩＤの認証子を生成して小容量版ＩＤに付加し，認証付きＩＤとする。認証子付きＩＤ設定手段６２は，無線タグ２１が有する大容量版ＩＤの個体番号に認証子付きＩＤを書き込み，また，大容量版ＩＤの製造者コードおよび商品種別コードのエリアに，代理サーバ７を送信先として特定することのできる商品情報とは無関係なコードを格納する。例えば製造者コードには，代理サーバ７を運営する第三者機関の会社コードを，商品種別コードには，ＩＤ認証サービスを示すコードを格納する。

【００１６】

クライアント３は，ＩＤ読み取り手段３１により，無線タグ２１から認証子付きＩＤを含む大容量版ＩＤを読み取り，ＩＤの製造者コードあるいは商品種別コードに基づき，転送先サーバ解決手段３２によって，アドレス解決サーバなどを別途利用するなどして，転送先サーバを決定する。ここで，無線タグ２１から読み取ったＩＤが，認証子付きＩＤを含む大容量版ＩＤの場合には，製造者コード，商品種別コードから代理サーバ７が転送先サーバとして選択されることになる。クライアント３は，認証子付きＩＤを含む大容量版ＩＤを代理サーバ７へ転送する。

【００１７】

代理サーバ７内の認証子付きＩＤ検証手段７１は，受信した認証子付きＩＤを検証し，正規ＩＤと判定した場合に，大容量版ＩＤから本来の小容量版ＩＤを抽出し，第１の本発明と同様に転送先サーバ解決手段７２によって転送先サーバのアドレス解決を行い，ＩＤ処理サーバ５へ本来の小容量版ＩＤを転送する。ＩＤ処理サーバ５の動作は，第１の本発明と同様である。

【００１８】

認証子付きＩＤ生成手段６１による小容量版ＩＤの認証子生成は，小容量版ＩＤの暗号処理（例えば，ＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｒｄ）生成，ディジタル署名など）により実現することができる。この認証子は，小容量版ＩＤをもとにＭＡＣやディジタル署名によって生成されたメッセージダイジェストであり，署名データになる。代理サーバ７は，元の小容量版ＩＤと認証子とを入力として，元の小容量版ＩＤが改竄されていないどうかを確認することができる。その認証に必要となる情報に，鍵を利用するアルゴリズムなどが必要であるが，これらの情報については，ＩＤ管理コンピュータ６と代理サーバ７との間で何らかの手段で共有しておく。共有方法は，安全に共有できる方法であればどのような方法でもよい。

【００１９】

また，小容量版ＩＤの認証子として，任意の認証子データを用意し，代理サーバ７において，本来の小容量ＩＤとその認証子データとの対応情報を管理し，クライアント３からの要求に応じて対応関係を検証する方法を用いることもできる。

【００２０】

第３の本発明は，上記第１の本発明と第２の本発明とを組み合せた手段を持つ発明である。ＩＤ管理コンピュータでは，本来の商品コードを示す小容量版ＩＤを秘匿化すると同時に，秘匿化した小容量版ＩＤの認証子を生成して，秘匿化した小容量版ＩＤに付加し，無線タグが有する大容量版ＩＤの個体番号のエリアに書き込み，また，大容量版ＩＤの製造者コードおよび商品種別コードのエリアに商品情報と無関係な送信先特定情報を格納する。この場合の送信先特定情報として，ＩＤの認証と秘匿化ＩＤの復号とを行う代理サーバが転送先サーバとして決定されるような情報を設定する。

【００２１】

以上のように，本発明によれば，本来のＩＤが秘匿化されて格納されているため，第三者により不正に読み取りされた場合でも，第三者は本来のＩＤを認識することができず，所有品情報などの漏洩を防ぐことが可能となる。また，本来のＩＤが認証子付きで格納されているため，代理サーバ７にて本来のＩＤの認証が可能となり，ＩＤの偽造やなりすましを防ぐことが可能となる。

【００２２】

【発明の実施の形態】
本発明をＭＩＴのオート（Ａｕｔｏ）ＩＤシステムに適用した例に従って，本発明の実施の形態を説明する。図３は，本発明の第１の実施の形態におけるシステムの全体構成の一例を示したものである。図３に示すシステムにおいて，１は小容量版ＩＤを秘匿化し，無線タグ２０の大容量版ＩＤ内に書き込むＩＤ管理コンピュータである。また，無線タグ２０は，商品２に貼られており，無線タグの読み取り装置３３を備えたクライアントコンピュータ３０と，ＩＤ（ＥＰＣ）データを格納するＰＭＬ（Ｐｈｙｓｉｃａｌ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）サーバ８と，ＩＤから，そのＩＤデータを格納するＰＭＬサーバ８のアドレスを解決するＯＮＳ（Ｏｂｊｅｃｔ　Ｎａｍｉｎｇ　Ｓｅｒｖｉｃｅ）サーバ９と，秘匿化ＩＤの復号処理などを行う代理サーバ４とが，インターネット１０により接続されている。
【００２３】
説明を簡単にするために，ここでは，秘匿化ＩＤの生成と秘匿化ＩＤを無線タグ２０に書き込む処理とを，１台のコンピュータによるＩＤ管理コンピュータ１で行う例を示しているが，秘匿化ＩＤを生成する処理とそれを無線タグ２０に書き込む処理とを分け，複数台のコンピュータによってＩＤ管理コンピュータ１を実現してもよい。
【００２４】
はじめに，本発明の第１の実施の形態に関するＥＰＣ（Ｅｌｅｃｔｒｏｎｉｃ　Ｐｒｏｄｕｃｔ　Ｃｏｄｅ）の格納方法を図４を用いて説明する。ＥＰＣは，ＡｕｔｏＩＤで用いるＩＤの名前である。ＥＰＣのコード体系として，種々のデータ長のものが規定されているが，本実施の形態では，９６ビット版ＥＰＣを本来のＩＤ，２５６版ＥＰＣを秘匿化ＩＤを含む大容量版ＩＤとして用いることにする。
【００２５】
図４（Ａ）に示す９６ビット版ＥＰＣは，バージョン番号８ビット，製造者コード２８ビット，商品種別コード２４ビット，個体番号３６ビットからなる。図４では，例として，“ＡＢＣ製薬”会社の製造者コード「０ｘ１２３４５６７」，“薬ＸＸ”の商品種別コード「０ｘＡＢＣＤＥＦ」，個体番号「０ｘ１２３４５６７８９」が格納されている様子を示している。
【００２６】
この状態のままでは，消費者が薬をカバンに入れ持ち歩いているとき，第三者が読み取り装置３３さえ持っていれば，ＥＰＣコードを読み取ることができ，その製造者コードと商品種別コードから，“ＡＢＣ製薬”の“薬ＸＸ”を所有しているということが第三者にわかってしまう。
【００２７】
本実施の形態では，図４（Ｂ）に示すように，ＩＤ管理コンピュータ１が，９６ビットの本来のＥＰＣを秘匿化し，図４（Ｃ）に示す２５６ビット版ＥＰＣの個体番号として格納する。秘匿化の例として，図４では，１２８ビット共通鍵暗号を利用している。このとき，２５６ビット版ＥＰＣの製造者コードおよび商品種別コードには，本来の商品のコードではなく，代理サーバ４をＥＰＣの送信先として特定することができるコードを設定する。図４（Ｃ）の例では，製造者コードとして代理サーバ４を運営する“プライバシ保護社”のコード「０ｘＡＢＣＤＥＦ０１２３４５６７８９」が格納され，また，商品種別コードとして，無線タグの“ＩＤ秘匿化サービス”のコード「０ｘ１２３４５６７８９０ＡＢＣＤ」が格納されている。
【００２８】
なお，秘匿化の方法として，公開鍵暗号を利用することも可能である。また，任意のコードを埋め込み，それと本来の９６ビット版ＥＰＣとの対応関係を代理サーバ４などに保有させておき，代理サーバ４にてＩＤ変換を行うという方法もある。すなわち，ＩＤ管理コンピュータ１と代理サーバ４との間で，任意のコードと９６ビット版ＥＰＣとの変換テーブルを何らの方法で共有し，その変換テーブルを用いてＩＤ変換を行う方法を用いてもよい。

【００２９】
さらに，図示していないが，秘匿化ＥＰＣの格納先として，個体番号領域だけでなく，商品種別コードの領域も合わせて利用することにより，より大きな秘匿化ＥＰＣデータをサポートすることもできる。また，商品種別コードに利用する秘匿化方法（暗号アルゴリズムや鍵ＩＤなど）を含めることにより，複数の暗号方法や鍵を扱えるようにすることも可能である。
【００３０】
次に，本発明の第１の実施の形態における本来の９６ビット版ＥＰＣのシステム全体の処理シーケンスについて，図５に従って説明する。図３のシステムにおいて，無線タグ２０内にＩＤ管理コンピュータ１が生成した２５６ビット版ＥＰＣではなく，図４（Ａ）に示す本来の９６ビット版ＥＰＣが格納されていた場合の処理シーケンスは，図５の（ａ１）～（ａ４）のようになる。この９６ビット版ＥＰＣの処理シーケンスでは，代理サーバ４が関与することがなく，シーケンスは従来技術とまったく同様である。
【００３１】
（ａ１）読み取り装置３３を内蔵した，クライアントコンピュータ３０が，無線タグ２０から本来の９６ビット版ＥＰＣを読み取る。
【００３２】
（ａ２）クライアントコンピュータ３０は，ＯＮＳサーバ９に対して，ＥＰＣを送信し，それを送信すべき転送先サーバのアドレスの解決要求を行う。
【００３３】
（ａ３）ＯＮＳサーバ９は，送信されてきたＥＰＣに基づき，ＰＭＬサーバ８のアドレスを回答する。このとき，製造者コードあるいは商品種別コードなどをアドレス解決に用いる。アドレス解決の結果，本来のＥＰＣの格納先であるＰＭＬサーバ８（製造メーカ管理など）のアドレスが返される。
【００３４】
（ａ４）クライアントコンピュータ３は，取得したアドレスに対して，ＥＰＣを送信する。ＰＭＬサーバ８は，受信したＥＰＣを内部データ（ＸＭＬ形式など）として保管する。
【００３５】
次に，本発明の第１の実施の形態におけるＥＰＣを秘匿化した場合（秘匿化ＥＰＣを２５６ビット版ＥＰＣの個体番号に格納）の処理シーケンスを，図６に示す（ｂ１）～（ｂ９）に従って説明する。
【００３６】
（ｂ１）読み取り装置３３を内蔵したクライアントコンピュータ３０が，秘匿化したＥＰＣを格納した２５６ビット版ＥＰＣ（図４（Ｃ））を，無線タグ２０から読み取る。
【００３７】
（ｂ２）クライアントコンピュータ３０は，ＯＮＳサーバ９に対して，２５６ビット版ＥＰＣを送信し，それを送信すべき転送先サーバのアドレスの解決要求を行う。
【００３８】
（ｂ３）ＯＮＳサーバ９は，送信されてきたＥＰＣの製造者コードあるいは商品種別コードに基づき，転送先サーバのアドレス（ここでは代理サーバ４のアドレス）を，要求元のクライアントコンピュータ３０に回答する。
【００３９】
（ｂ４）クライアントコンピュータ３０は，取得したアドレスに対して，秘匿化ＥＰＣを含む２５６ビット版ＥＰＣを送信する。
【００４０】
（ｂ５）代理サーバ４は，受信した２５６ビット版ＥＰＣから，秘匿化された９６ビット版ＥＰＣを取り出す。
【００４１】
（ｂ６）代理サーバ４は，秘匿化ＥＰＣを復号することにより，本来の９６ビット版ＥＰＣを得る。

【００４２】
（ｂ７）次に，代理サーバ４は，本来のＥＰＣをＯＮＳサーバ９へ送信し，対応する転送先サーバのアドレス解決要求を行う。
【００４３】
（ｂ８）ＯＮＳサーバ９は，受け取ったＥＰＣの製造者コードあるいは商品種別コードに基づき，本来のＥＰＣを処理するＰＭＬサーバ８のアドレスを得て，そのＰＭＬサーバ８のアドレスを代理サーバ４に回答する。
【００４４】
（ｂ９）代理サーバ４は，そのＰＭＬサーバ８に対して本来のＥＰＣを送信し，ＰＭＬサーバ８は受信したＥＰＣを内部データ（ＸＭＬ形式など）として保管する。
【００４５】
ここで，クライアントコンピュータ３０と代理サーバ４間は，クライアント認証付きのＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）　など，アクセス制御や通信路の暗号化，改竄検出などセキュアな通信路が別手段として提供されているものとする。
【００４６】
次に，本発明をＭＩＴのオート（Ａｕｔｏ）ＩＤシステムに適用した第２の実施の形態を説明する。第２の実施の形態のシステム構成を，図７に示す。第２の実施の形態においても，基本的な構成は第１の実施の形態と同様である。第１の実施の形態との違いは，ＩＤ管理コンピュータ６が９６ビット版ＥＰＣに認証子を付けることにより２５６ビット版ＥＰＣを生成し，無線タグ２１に設定すること，代理サーバ７が，２５６ビット版ＥＰＣの認証子付きＩＤを検証することにより，無線タグ２１から読み取ったＥＰＣが正規ＩＤであることを検証することである。
【００４７】
本発明の第２の実施の形態に関するＥＰＣの格納方法を，図８を用いて説明する。図８（Ａ）に示す９６ビット版ＥＰＣは，ＭＩＴのオート（Ａｕｔｏ）ＩＤシステムで規定された本来の小容量版ＥＰＣであり，バージョン番号８ビット，製造者コード２８ビット，商品種別コード２４ビット，個体番号３６ビットからなる。図８では，例として，“ＡＢＣバッグ”会社の製造者コード「０ｘ２３４５６７８」，“バッグＸＸ”の商品種別コード「０ｘＢＣＤＥＦＧ」，個体番号「０ｘ２３４５６７８９１」が格納されている様子を示している。
【００４８】
本実施の形態では，図８（Ｂ）に示すように，ＩＤ管理コンピュータ６が，本来の９６ビット版ＥＰＣの認証子を生成する。この例では，認証子の生成に，ハッシュ関数の一つであるｓｈａ１（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ　１）　を用い，ｓｈａ１の出力１６０ビットから６４ビット分を切り出して，６４ビットの認証子を生成している。ＩＤ管理コンピュータ６は，本来の９６ビット版ＥＰＣに，生成した６４ビットの認証子を付加し，図８（Ｃ）に示す２５６ビット版ＥＰＣの個体番号として格納する。
【００４９】
このとき，２５６ビット版ＥＰＣの製造者コードおよび商品種別コードには，本来の商品のコードではなく，代理サーバ７をＥＰＣの送信先として特定することができるコードを設定する。図４（Ｃ）の例では，製造者コードとして代理サーバ７を運営する“真贋判定社”のコード「０ｘＢＣＤＥＦＧ０１」が格納され，また，商品種別コードとして，“ＩＤ認証サービス”のコード「０ｘ２３４５６７８９１０ＢＣＤＥ」が格納されている。
【００５０】
なお，本システムにおいては，上記認証子の生成を暗号処理（例えば，ＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｒｄ）　生成，ディジタル署名）により実現することも可能であり，また，認証子として任意のコードを用意し，それと本来のＥＰＣとの対応関係を代理サーバ７に保有させておき，代理サーバ７にて対応関係を検証するという方法を採ることも可能である。
【００５１】

次に，本発明の第２の実施の形態におけるＥＰＣに認証子を付加した場合（認証子付きＥＰＣを２５６ビット版ＥＰＣの個体番号に格納）の処理シーケンスを，図９に示す（ｃ１）～（ｃ９）に従って説明する。

【００５２】

（ｃ１）読み取り装置３３を内蔵したクライアントコンピュータ３０が，認証子付きＥＰＣを格納した２５６ビット版ＥＰＣ（図８（Ｃ））を，無線タグ２１から読み取る。

【００５３】

（ｃ２）クライアントコンピュータ３０は，ＯＮＳサーバ９に対して，２５６ビット版ＥＰＣを送信し，それを送信すべき転送先サーバのアドレスの解決要求を行う。

【００５４】

（ｃ３）ＯＮＳサーバ９は，送信されてきたＥＰＣの製造者コードあるいは商品種別コードに基づき，転送先サーバのアドレス（ここでは代理サーバ７のアドレス）を回答する。

【００５５】

（ｃ４）クライアントコンピュータ３０は，取得したアドレスに対して，認証子付きＥＰＣを含む２５６ビット版ＥＰＣを送信する。

【００５６】

（ｃ５）代理サーバ７は，受信した２５６ビット版ＥＰＣから，認証子付きＥＰＣを取り出す。

【００５７】

（ｃ６）代理サーバ７は，認証子付きＥＰＣを認識子に基づいて検証する。

【００５８】

（ｃ７）代理サーバ７は，上記検証の結果，正規ＩＤと判断した場合に，ＯＮＳサーバ９に対して認証子付きＥＰＣの中の本来の９６ビット版ＥＰＣを送り，転送先サーバのアドレス解決要求を行う。

【００５９】

（ｃ８）ＯＮＳサーバ９は，受け取った９６ビット版ＥＰＣにおける製造者コードあるいは商品種別コードから，本来のＥＰＣを処理するＰＭＬサーバ８のアドレスを回答する。

【００６０】

（ｃ９）代理サーバ７は，そのＰＭＬサーバ８に対して本来のＥＰＣを送信し，ＰＭＬサーバ８は受信したＥＰＣを内部データ（ＸＭＬ形式など）として保管する。

【００６１】

本発明の第３の実施の形態では，上記第１の実施の形態におけるＥＰＣの秘匿化と，第２の実施の形態における認証子の付加とを同時に行う。システム構成については，図３および図７と同様である。第３の実施の形態におけるＩＤ管理コンピュータの処理フローチャートを，図１０に示す。

【００６２】

ステップＳ１では，ＩＤ管理コンピュータは，無線タグの添付対象となる商品を識別する本来の９６ビット版ＥＰＣを入力する。次に，ステップＳ２では，入力した本来の９６ビット版ＥＰＣを所定の共通鍵または公開鍵などを用いて暗号化し，秘匿化ＥＰＣを生成する。ステップＳ３では，秘匿化ＥＰＣについてＭＡＣ生成やディジタル署名などの暗号処理により，認証子を生成する。

【００６３】

ステップＳ４では，ステップＳ２，Ｓ３で生成した秘匿化ＥＰＣと認証子とを，２５６ビット版ＥＰＣの個体番号とする。ステップＳ５では，ＩＤ認証・秘匿化サービスに対してあらかじめ付与した固有の番号を，２５６ビット版ＥＰＣにおける商品種別コードとする。ステップＳ６では，代理サーバの運営会社に対してあらかじめ付与した固有の番号を，２５６ビット版ＥＰＣにおける製造者コードとする。なお，代理サーバの運営会社の番号およびＩＤ認証・秘匿化サービスの番号と，代理サーバのアドレス（ＩＰアドレス）との対応情報は，あらかじめＯＮＳサーバに登録しているものとする。

【００６４】

ステップＳ７では，ＥＰＣの世代またはデータ長などの種別を示すバージョン番号と，ステップＳ６で決定した製造者コードと，ステップＳ５で決定した商品種別コードと，ステップＳ４で決定した個体番号とを結合して，２５６ビット版ＥＰＣを生成する。ステップＳ８では，生成した２５６ビット版ＥＰＣを無線タグに書き込み，一つの無線タグへの書き込み処理を終了する。

【００６５】

第３の実施の形態における代理サーバの処理フローチャートを，図１１に示す。ステップＳ１０では，クライアントコンピュータが無線タグから読み取った秘匿化ＥＰＣと認証子とを含む２５６ビット版ＥＰＣを受信する。ステップＳ１１では，受信した２５６ビット版ＥＰＣの個体番号から認証子を切り出し，正当なＩＤかどうかを検証する。ステップＳ１２の判定により，検証した結果が正当でなければ，ステップＳ１３へ進み，２５６ビット版ＥＰＣの送信元であるクライアントコンピュータへエラー通知を行い，処理を終了する。

【００６６】

検証した結果，正当なＩＤであることがわかれば，ステップＳ１４へ進み，２５６ビット版ＥＰＣの個体番号から秘匿化ＥＰＣを切り出して復号することにより，本来の９６ビット版ＥＰＣを復元する。ステップＳ１５では，９６ビット版ＥＰＣをＯＮＳサーバへ送り，９６ビット版ＥＰＣの製造者コード，商品種別コードによって定まるＰＭＬサーバのアドレスを得る。ステップＳ１６では，ＰＭＬサーバへ９６ビット版ＥＰＣを送信し，処理を終了する。

【００６７】

以上説明したＩＤ管理コンピュータおよび代理サーバの処理は，コンピュータとソフトウェアプログラムとによって実現することができ，そのプログラムをコンピュータ読み取り可能な記録媒体に記録して提供することも，ネットワークを通して提供することも可能である。

【００６８】

【発明の効果】

以上説明したように，本発明によれば，無線タグには，添付対象を識別する本来のＩＤが秘匿化されて格納されており，その復号は，正規のコンピュータである代理サーバが自動的に呼び出されて行う仕組みを持つことにより，不正な第三者に対する無線タグのＩＤ情報漏洩を防止することができ，所有品情報などに関するプライバシを保護することが可能となる。また，認証子付きのＩＤを格納することにより，ＩＤが不正に生成され偽造商品などに貼り付けられている場合にも，ＩＤ偽造の検出が可能となり，偽造防止などが可能となる。

【図面の簡単な説明】

【図１】本発明の構成の一例を示す図である。

【図２】本発明の構成の一例を示す図である。

【図３】第１の実施の形態におけるシステムの全体構成の一例を示す図である。

【図４】秘匿化ＩＤの格納方法を説明する図である。

【図５】本来の９６ビット版ＥＰＣの処理シーケンスを示す図である。

【図６】秘匿化ＩＤを含む２５６版ＥＰＣの処理シーケンスを示す図である。

【図７】第２の実施の形態におけるシステムの全体構成の一例を示す図である。

【図８】認証子付きＩＤの格納方法を説明する図である。

【図９】認証子付きＩＤの処理手順を説明するシーケンス図である。

【図１０】第３の実施の形態におけるＩＤ管理コンピュータの処理フローチャートである。

【図１１】第３の実施の形態における代理サーバの処理フローチャートである。

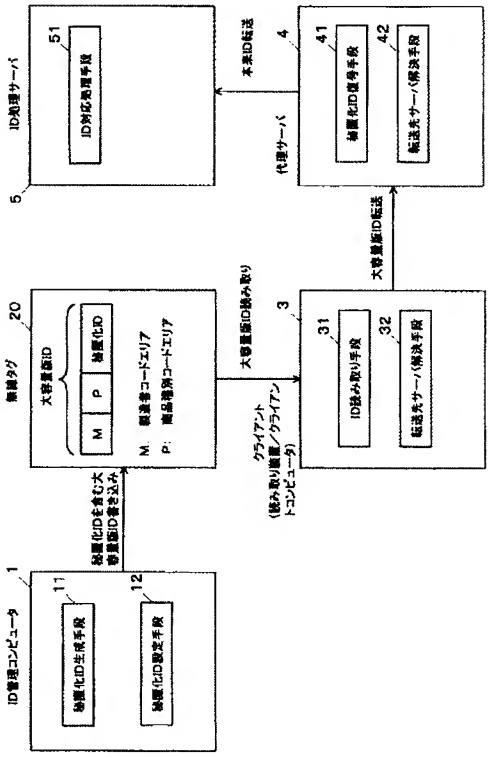
【符号の説明】

１，６　ＩＤ管理コンピュータ

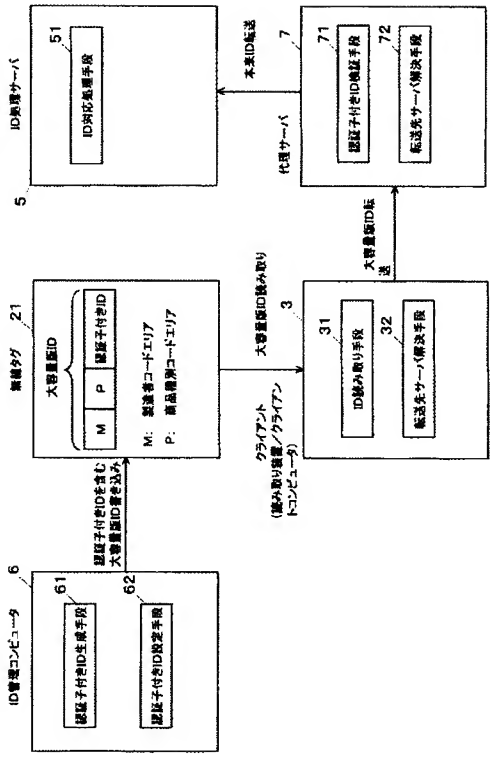
２　商品

３　クライアントコンピュータ
４，７　代理サーバ
５　ＩＤ処理サーバ
８　ＰＭＬサーバ
９　ＯＮＳサーバ
１０　インターネット
１１　秘匿化ＩＤ生成手段
１２　秘匿化ＩＤ設定手段
２０，２１　無線タグ
３０　クライアントコンピュータ
３１　ＩＤ読み取り手段
３２，４２，７２　転送先サーバ解決手段
３３　読み取り装置
４１　秘匿化ＩＤ復号手段
５１　ＩＤ対応処理手段
６１　認証子付きＩＤ生成手段
６２　認証子付きＩＤ設定手段
７１　認証子付きＩＤ検証手段

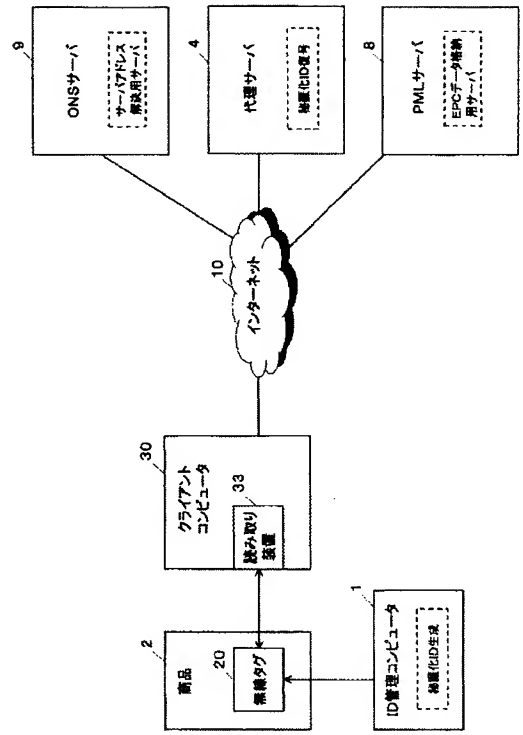
【図1】



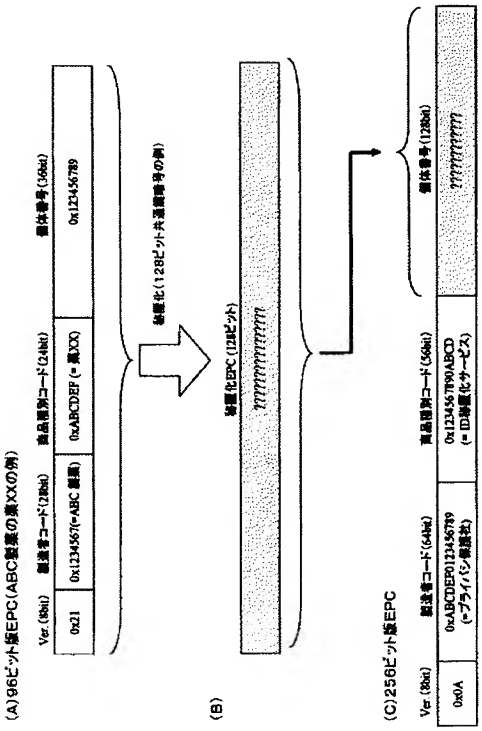
【図2】



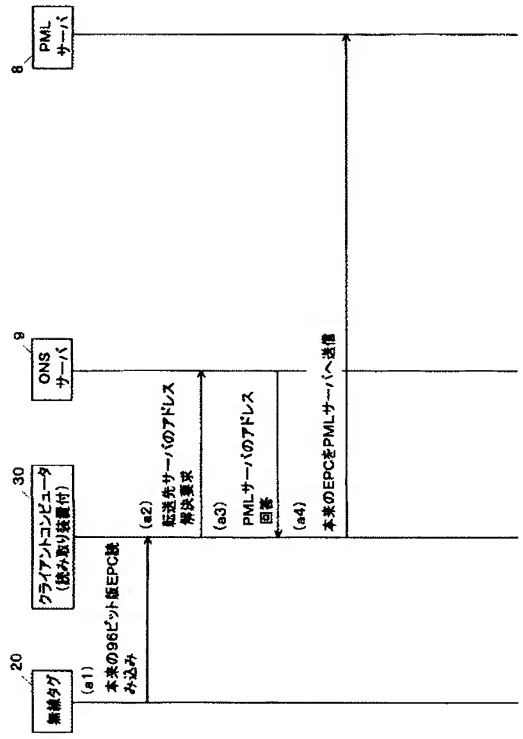
【図3】


9
ONSサーバ
サーバアドレス解決用サーバ
4
代理サーバ
暗号化ID復号
8
PMLサーバ
EPCデータ格納用サーバ
10
インターネット
30
クライアントコンピュータ
33
読み取り装置
2
商品
20
無線タグ
1
ID管理コンピュータ
暗号化ID生成

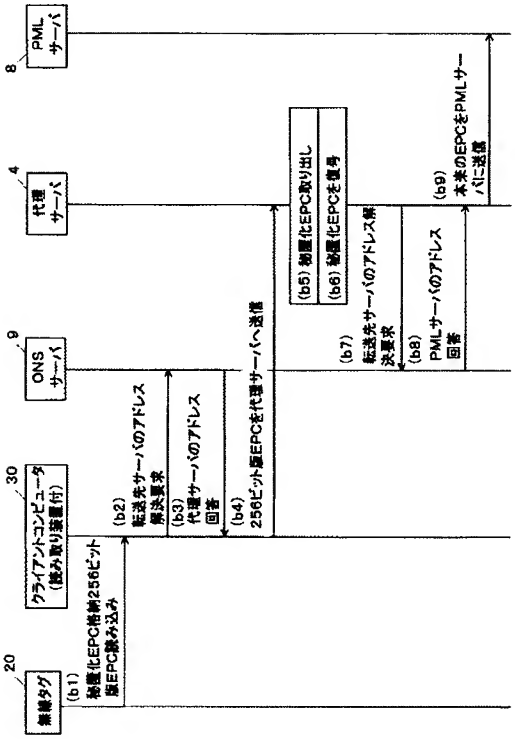
【図4】


(A)96ビット版EPC(ABC製薬の薬XXの例)
Ver (8bit)
0x21
製造者コード(28bit)
0x12345670(=ABC 製薬)
商品種別コード(24bit)
0xABCDEF (= 薬XX)
個体番号(36bit)
0x123456789
暗号化(128ビット共通鍵暗号の例)
(B)
暗号化EPC (128ビット)
???????????????
(C)256ビット版EPC
Ver (8bit)
0x0A
製造者コード(64bit)
0xABCDEF0123456789
(=プライバシー保護型)
商品種別コード(56bit)
0x12345678900ABCD
(= ID暗号化サービス)
個体番号(128bit)
???????????????

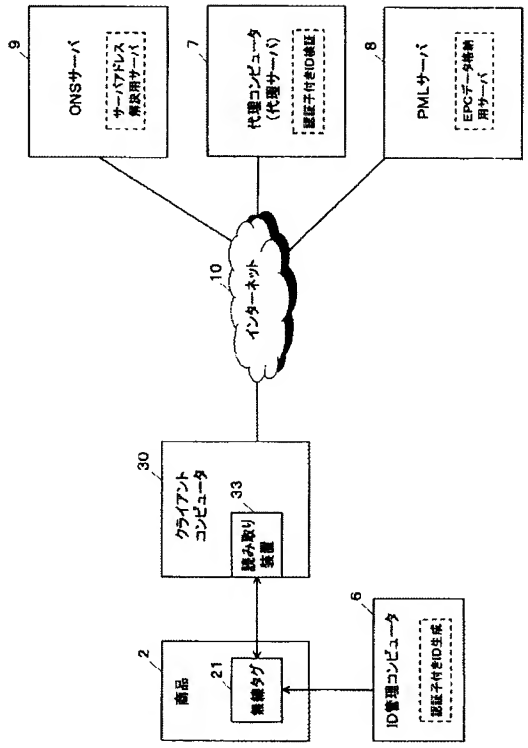
【図5】


8
PMLサーバ
9
ONSサーバ
30
クライアントコンピュータ(読み取り装置付)
20
無線タグ
(a1)
本来の96ビット版EPC読み込み
(a2)
転送先サーバのアドレス解決要求
(a3)
PMLサーバのアドレス回答
(a4)
本来のEPCをPMLサーバへ送信

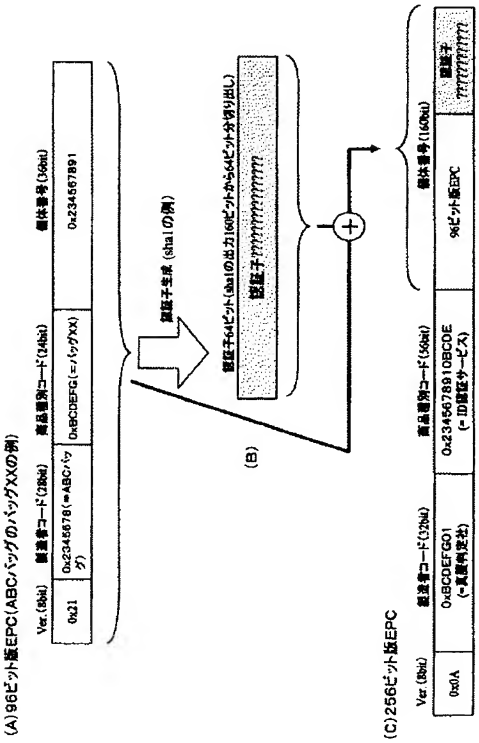
【図6】


8
PMLサーバ
4
代理サーバ
9
ONSサーバ
30
クライアントコンピュータ(読み取り装置付)
20
無線タグ
(b1)
暗号化EPC格納256ビット版EPC読み込み
(b2)
転送先サーバのアドレス解決要求
(b3)
代理サーバのアドレス回答
(b4)
256ビット版EPCを代理サーバへ送信
(b5) 暗号化EPC取り出し
(b6) 暗号化EPCを復号
(b7)
転送先サーバのアドレス解決要求
(b8)
PMLサーバのアドレス回答
(b9)
本来のEPCをPMLサーバに送信

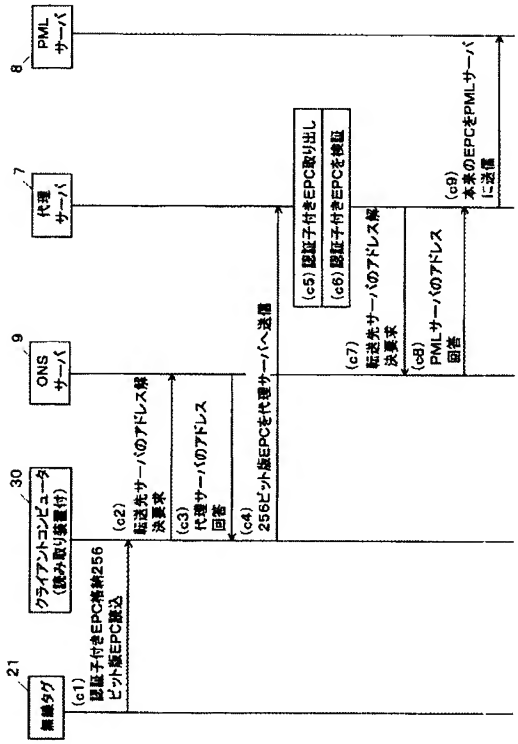
【図7】


9
ONSサーバ
サーバアドレス解決用サーバ
7
代理コンピュータ（代理サーバ）
認証子付きID検証
8
PMLサーバ
EPCデータ格納用サーバ
10
インターネット
30
クライアントコンピュータ
33
読み取り装置
2
商品
21
無線タグ
6
ID管理コンピュータ
認証子付きID生成

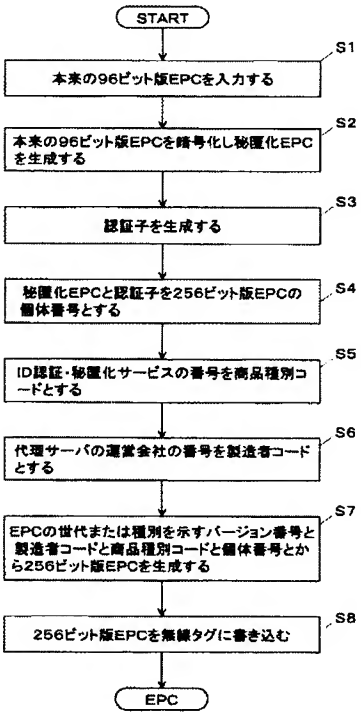
【図8】


(A)96ビット版EPC(ABCバッグのバッグXXの例)
Ver.(8bit)
0x21
製造者コード(28bit)
0x2345678(=ABCバッグ)
商品種別コード(24bit)
0xBCDEFG(=バッグXX)
個体番号(36bit)
0x234567891
認証子生成（sha1の例）
(B)
認証子64ビット(sha1の出力160ビットから64ビット分切り出し)
認証子????????????????
(C)256ビット版EPC
Ver.(8bit)
0x0A
製造者コード(32bit)
0xBCDEFG01
(=真贋株式会社)
商品種別コード(56bit)
0x2345678910BCDE
(=ID認証サービス)
個体番号(160bit)
96ビット版EPC
認証子
????????

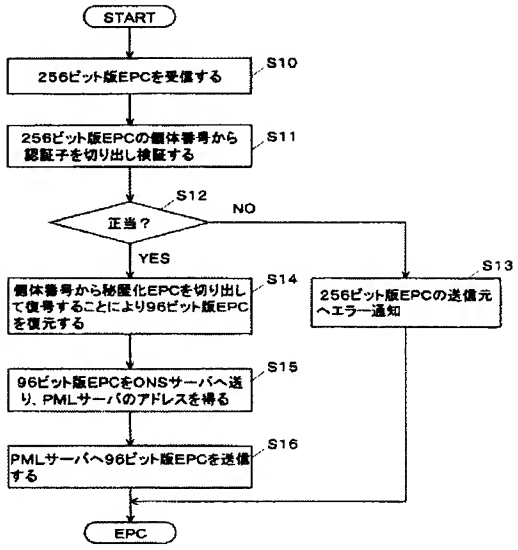
【図9】


8
PMLサーバ
7
代理サーバ
9
ONSサーバ
30
クライアントコンピュータ（読み取り装置付）
21
無線タグ
(c1)
認証子付きEPC格納256ビット版EPC読込
(c2)
転送先サーバのアドレス照会決要求
(c3)
代理サーバのアドレス回答
(c4)
256ビット版EPCを代理サーバへ送信
(c5)
認証子付きEPC取り出し
(c6)
認証子付きEPCを検証
(c7)
転送先サーバのアドレス照会決要求
(c8)
PMLサーバのアドレス回答
(c9)
本来のEPCをPMLサーバに送信

【図10】


START
S1
本来の96ビット版EPCを入力する
S2
本来の96ビット版EPCを暗号化し秘匿化EPCを生成する
S3
認証子を生成する
S4
秘匿化EPCと認証子を256ビット版EPCの個体番号とする
S5
ID認証・秘匿化サービスの番号を商品種別コードとする
S6
代理サーバの運営会社の番号を製造者コードとする
S7
EPCの世代または種別を示すバージョン番号と製造者コードと商品種別コードと個体番号とから256ビット版EPCを生成する
S8
256ビット版EPCを無線タグに書き込む
EPC

【図11】


START
256ビット版EPCを受信する
S10
256ビット版EPCの個体番号から認証子を切り出し検証する
S11
正当？
S12
NO
YES
個体番号から秘匿化EPCを切り出して復号することにより96ビット版EPCを復元する
S14
256ビット版EPCの送信元へエラー通知
S13
96ビット版EPCをONSサーバへ送り、PMLサーバのアドレスを得る
S15
PMLサーバへ96ビット版EPCを送信する
S16
EPC

(72)発明者　小室　智之
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　藤村　明子
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考) 5B058 CA01 CA15 KA32 KA33 YA20
5J104 AA07 KA02 KA04 KA15 NA02 NA05 NA27 NA38 PA07 PA10